„Bieten Werkzeuge und Expertise“

Dr. Philipp Amann, Cybercrime-Experte bei Europol, über Internetkriminalität während der Pandemie, den Erfolg internationaler Polizeizusammenarbeit und die Bedeutung einer „Grundhygiene“ im Cyberspace.

Wofür ist das Zentrum zur Bekämpfung der Cyber-Kriminalität bei Europol zuständig?

Innerhalb der EU-Strafverfolgungsbehörde Europol ist das *European Cybercrime Centre (EC3)* dazu da, die nationalen Strafverfolgungsbehörden bei der Bekämpfung von Cyber-Kriminalität zu unterstützen und dadurch letztlich auch Bürgerinnen und Bürger, Unternehmen und Regierungen vor solchen Angriffen zu schützen. *EC3* ist eines von mehreren Kompetenzzentren bei Europol mit besonderen operativen und strategischen Schwerpunkten.

Dazu gehören auch das *European Counter-Terrorism-Centre (ECTC)* zur Terrorbekämpfung, das *European Migrant-Smuggling-Centre (EMSC)* zur Schleppereibekämpfung, das *European Serious-Organised-Crime-Centre (ESOCC)* gegen organisierte Kriminalität und, seit letztem Jahr, das *European Financial and Economic-Crime-Center (EFECC)*. Dieses wird von dem Österreicher Burkhard Mühl geleitet.

Wie kann man sich die Arbeit im EC3 vorstellen?

Die Arbeit innerhalb des Zentrums gliedert sich in drei Hauptbereiche – den operativen Bereich, den Bereich für Dokumenten- und Digitalforensik und den Bereich für Expertise und Stakeholder-Management, in dem ich als Referatsleiter tätig bin. Hier soll die Arbeit zwischen öffentlichen und privaten Akteuren koordiniert und unterstützt werden. Als „Head of Strategy“ im *EC3* kümmere ich mich zudem um Präventions- und Bewusstseinsbildung sowie die Analyse und strategische Bewertung von aktuellen und künftigen Bedrohungen in Bezug auf Cyberkriminalität. Dazu erstellen wir beispielsweise Berichte. Der zentrale Bericht des *EC3* ist die jährliche Einschätzung von weitreichenden Cybercrime-Bedrohungen für die EU, das *Internet Organised Crime Threat Assessment (IOCTA)*.

Wo liegen die Schwerpunkte des EC3 im operativen Bereich?

Wir haben vier Schwerpunkte gesetzt, auf die wir uns bei der Cyber-Kriminalität im Moment besonders konzentrieren: Hightech-Verbrechen, den sexuellen Missbrauch von Kindern, das Darknet und Formen des Finanzbetrugs, wenn sie online passieren. Hier gibt es, so wie in manchem anderen Bereich, Überlappungen mit anderen Zentren. Ein eigenes Team ist zudem mit der Zusammenführung sensibler Informationen, also mit „Intelligence“, befasst. Eine wichtige operative Vernetzung innerhalb des *EC3* erfolgt im Rahmen der *Joint Cybercrime Action Taskforce (J-CAT)*, die an das *EC3* angegliedert ist. Österreich war 2014 einer der Mitbegründer dieser Taskforce. Die Idee dahinter war, innerhalb von Europol – neben der bewährten Kooperation der im Grunde für alle Fragen zuständigen Verbindungsbeamten – ein eigenes Netzwerk zu bilden, das ausschließlich aus Expertinnen und Experten für Cyber-Kriminalität besteht.

Philipp Amann: „Klärung vieler kleiner Verbrechen ist oft der größte Erfolg.“

Wie wird in der Joint Cybercrime Action Taskforce kooperiert?

Im Moment sind 16 Staaten mit dem *EC3* in der *Joint Cybercrime Action Taskforce*. Dabei handelt es sich um neun EU-Staaten, darunter auch Österreich, und sieben Drittstaaten. Den Vorsitz führen zur Zeit die Niederlande, den Vize-Vorsitz nimmt ein Nicht-EU-Staat, die Schweiz, wahr. Aus meiner Sicht ist das *J-CAT* eine der wichtigsten operativen Plattformen zur Zusammenarbeit von Strafverfolgungsbehörden bei Europol im Kampf gegen die Cyber-Kriminalität . Wir haben auch die USA mit dem *FBI* und dem *Secret Service* und Dienststellen aus Kanada, Australien oder Kolumbien an Bord. Eine derartig gelungene Kooperation ist einmalig: Die Spezialistinnen und Spezialisten sitzen physisch zusammen, priorisieren Meldungen, versuchen, Konflikte zu verhindern und initiieren grenzüberschreitende Ermittlungen. Bei den meisten großen Cybercrime-Fällen, die Europol unterstützt hat, war die *J-CAT* beteiligt. Österreich hat die Bedeutung dieser Taskforce früh erkannt – und auch, wie wichtig die Kooperation über die EU-Grenzen hinaus und mit der Privatwirtschaft ist. Wenn man sich ansieht, wo Europol am erfolgreichsten ist, so erkennt man immer wieder, dass es sich um die fachlichen Netzwerke handelt. Hier sind das Wissen und das Vertrauen vorhanden, um schnell und effektiv vorzugehen. Dabei müssen mit der Arbeit in den Zentren nicht immer nur die „ganz großen Fische“ gefangen werden – oft ist die Klärung vieler kleiner Verbrechen der größte Erfolg.

ZUR PERSON

Der Österreicher Dr. Philipp Amann ist Head of Strategy beim European Cybercrime Centre (EC3) von Europol in Den Haag. Vor seiner Tätigkeit bei Europol ab 2013 war Philipp Amann unter anderem beim Internationalen Strafgerichtshof in Den Haag, der Organisation for the Prohibition of Chemical Weapons in Den Haag und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) in Wien tätig. Bei der OSZE war er bereits für den Bereich Cybercrime zuständig. Amann hat ein Doktorat in Wirtschaftsinformatik an der Universität Wien und einen Master of Science (MSc) in Forensic Computing and Cybercrime Investigation am University College Dublin erworben.

FOTO: EUROPOL

Sie haben den Arbeitsschwerpunkt „Darknet“ im EC3 angesprochen?

Ja, im *EC3* besteht dafür ein eigenes Team. Der Kampf gegen die kriminellen Vorgänge im Darknet wird als Priorität definiert, internationale Strategie sollen vorangetrieben werden. Europol will grenzüberschreitende Operationen unterstützen, aber auch die Kooperation mit der Industrie oder mit Firmen für Kryptowährung fördern. Zuletzt war allerdings einen Trend weg von zentralen Marktplätzen zu beobachten, auch als Reaktion Krimineller auf erfolgreiche Operationen von Ermittlungsbehörden. In Plattformen wie *Discord, Wickr* und *Telegram* findet ein ständiges „Katz- und Mausspiel“ statt. Abhängig vom jeweiligen Betreiber von Chatplattformen lassen sich Nachrichten nicht immer mit Hilfe des Betreibers auslesen, weil er den Schlüssel selbst nicht hat.

Cyber-Kriminelle haben inzwischen oft ein hohes Wissen zu Anonymisierung und eigener „Betriebssicherheit“ und es braucht eine Reihe von Maßnahmen – von neuester Technik bis zu neuen operativen Strategien – um erfolgreich zu sein. Zuletzt war die Operation „Trojan Shield“ ein gutes Beispiel, bei der das *FBI* in Koordination mit australischen Behörden ein verschlüsseltes Kommunikationsnetzwerk namens *ANOM* für die Benutzung von Kriminellen entwickelt hat.

Wann kann Europol um Unterstützung gebeten werden?

Im Regelfall müssen zumindest zwei oder mehr Mitgliedstaaten betroffen sein, damit Europol tätig werden kann. Allerdings ist dazu immer die Anforderung eines Mitgliedstaates notwendig, denn Europol selbst hat keine Polizeibefugnisse und startet auch keine eigenen Ermittlungsverfahren. Was wir beispielsweise anbieten können, sind Expertise oder Werkzeuge, die auf nationaler Ebene nicht unbedingt vorhanden sind. Wir können etwa Zugang zu verschlüsselten Handys ermöglichen, in die Dienststellen in einem Mitgliedstaat nicht hineingekommen sind, oder wir erhalten verschlüsselte Festplatten, wo wir oft den Zugriff auf relevante Ermittlungsdaten für Mitgliedstaaten bereitstellen können. Hier spielt der breite Bereich der Digital-Forensik hinein, der etwa auch das Auslesen von Computerdaten in Fahrzeugen umfasst. Speziell bei komplexen Aufgabenstellungen entsenden wir, wenn angefordert, zum Teil auch Europol-Experten. Informationen können über das Europol-System *SIENA* sicher und datenschutzkonform ausgetauscht werden. Neben dem *J-CAT* gibt es zahlreiche weitere sehr erfolgreiche Netzwerke, um Probleme zu lösen und adäquate Antworten zu finden – zum Beispiel die *European Union Cybercrime Taskforce (EUCTF),* die es schon vor dem *EC3* gegeben hat. In der *EUCTF* sind die Leiter der verschiedenen Cybercrime-Abteilungen aller Mitgliedstaaten vertreten, die zweimal im Jahr mit Repräsentanten von Europol, Eurojust und der Europäischen Kommission zusammenkommen.

Philipp Amann: „Die Cyber-Kriminalität befindet sich nicht mehr in einem Stadium der Revolution, sondern der Evolution.“

Wie verlaufen die Kontakte zwischen EC3 und Österreich?

Die zentrale Drehscheibe ist das österreichische Verbindungsbüro des Innenministeriums bei Europol unter der Leitung von Dr. Christian Wandl. Der nationale Kontaktpunkt ist das *Cyber-Crime-Competence-Center C4* im Bundeskriminalamt, über das der direkte und sichere Austausch erfolgt. Das können kurze und einfache Anfragen sein, die Bitte um Unterstützung in einem Ermittlungsverfahren oder der Austausch von Informationen im Rahmen eines multilateralen Verfahrens. Österreich ist kein großes Land, aber wir haben in bestimmten Bereichen große Expertise, zum Beispiel bei Kryptowährungen. Da können andere Staaten profitieren.

Das EC3 ist 2013 gegründet worden. Wie hat sich die Cyber-Kriminalität in den letzten 8 Jahren weiterentwickelt?

Ein wichtiger Bereich der Arbeit des *EC3* sind Analysen. Im Rahmen der Trendanalyse des „Internet Organised Crime Threat Assessment“, unseres wichtigsten jährlichen Produkts, haben wir letztes Jahr festgehalten, dass sich die Cyber-Kriminalität nicht mehr in einem Stadium der Revolution, sondern der Evolution befindet. Die „Untergrundindustrie“ hat ihre Taktiken professionalisiert und zuletzt, etwa in der Corona-Pandemie, sehr flexibel angepasst. Ein Beispiel ist der Bereich der Ransomware, also der Einsatz von Schadsoftware, mit der in ein Computersystem eingedrungen wird, um dann quasi ein ‚Lösegeld‘ zu verlangen. Im Fünfjahres-Rückblick sieht man die Evolution: Anfangs wurde nur der Zugang zum Computer geblockt, dann wurden die Daten verschlüsselt. Inzwischen haben die Kriminellen ihre Methoden weiter verfeinert und kopieren die Daten vor der Verschlüsselung. Es wird dann mit der Veröffentlichung der Daten bei Nichtbezahlung gedroht. Cyber-Kriminelle wissen, wie sie sich selbst schützen und agieren arbeitsteilig. Mit Gelegenheitsverbrecher haben wir es hier kaum mehr zu tun.

Welchen Einfluss hatte die Corona-Pandemie auf Verbrechen im Internet?

Soweit wir es beobachten konnten, ist die Pandemie von Cyber-Kriminel-

FOTO: EUROPOL

len schnell als Möglichkeit verstanden worden, die Krise für ihre Angriffe zu verwenden und neue „Geschäftsbereiche“ zu erschließen. So sind schon nach kurzer Zeit etwa im Darknet gefälschte Testkits und Masken angeboten worden. Die berüchtigten Scamming-Mails, in denen betrügerische Inhalte verpackt sind, haben eine neue Qualität erreicht, zum Beispiel gefälschte Versandnachrichten von angeblichen Paketzusendungen. Oder man denke an komplizierte Fremdsprachen wie Finnisch, in denen früher kaum Scammings ausgeschickt wurden, weil man die Fälschung durch die fehlerhaften Texte sofort erkannt hätte. Inzwischen sind diese Mails so gut verfasst, zum Beispiel in perfektem Finnisch, dass man extrem aufpassen muss, nicht getäuscht zu werden – die Übersetzungsdienste werden in der ‚Untergrundindustrie‘ angeboten. Bestürzend ist auch, wie die Zahl der Zugriffe auf Kindesmissbrauchsmaterial im Internet in die Höhe geschnellt ist.

Wie kann man gegensteuern, dass die zunehmende Digitalisierung nicht zu mehr Cyber-Kriminalität führt?

Die Digitalisierung hat viele Vorteile, sie macht unser Leben einfacher. Gerade in der Pandemie hat sich auch gezeigt, dass es vielen Menschen Dank der Digitalisierung möglich war, weiterzuarbeiten, Kontakte und Interessen zu pflegen. Durch die Expansion des Internets gibt es aber immer mehr Angriffsflächen. Denken Sie nur an Alltagsgeräte wie Küchengeräte oder Spielzeug, die plötzlich online sind – Stichwort „Internet of Things“. Ich halte es daher für wesentlich, dass jede Nutzerin und jeder Nutzer eine gewisse „Grundhygiene“ im Cyberspace einhält, um sich vor Cyber-Kriminalität zu schützen. Dazu gehört, dass sich Privatpersonen eine Antivirensoftware besorgen, regelmäßig Updates auf ihren Geräten herunterladen, Back-ups ihrer Daten erstellen oder sich bewusst machen, dass man nicht auf jeden Link klicken sollte. Hier gibt es eine gewisse Eigenverantwortung.

In Unternehmen kann man in der Regel noch viel mehr machen, um einen ausreichenden Schutz aufzubauen, man muss aber auch bereit sein, etwas zu investieren. Es gilt für mich immer noch der Spruch: „Wenn ich mich als Firma nicht professionell mit möglichen IT-Schwachstellen beschäftigte, macht es

Europol ist die Strafverfolgungsbehörde der Europäischen Union mit Sitz in Den Haag.

ein Krimineller ‚gratis‘ für mich.“ Ich sehe aber auch bei der Industrie eine spezielle Verantwortung. Wenn neue Software und Hardware entwickelt werden, sollten die Sicherheitsaspekte immer mitbedacht werden und Teil des Produktdesigns sein. Man sollte sich nicht nur auf neue Features konzentrieren, sondern auch überlegen, welche Risiken dadurch entstehen und wie diese abgefangen werden können. Oft können relativ einfache Maßnahmen schon eine große Wirkung haben. Ein gutes Beispiel ist die Multifaktorauthentifizierung bei Passwörtern. Wir haben gesehen, dass dort, wo sie eingesetzt wird, Kriminelle sich lieber andere Ziele aussuchen, in die sie leichter hineinkommen.

Kürzlich hat ein Cyber-Angriff auf eine Pipeline in den USA die Schlagzeilen dominiert. Welchen Lehren kann Europa aus diesem Fall ziehen?

Das Thema hat die U.S.-Medien besonders stark beherrscht, weil größere Ausfälle in der Treibstoffversorgung befürchtet wurden. Fast zur gleichen Zeit gab es aber auch in Europa einen aufsehenerregenden Cyber-Angriff – und zwar auf das IT-Systeme irischer Krankenhäuser. So wie in den USA handelte es sich um einen Fall mit Ransomware. Diese Angriffe hatten also Auswirkungen auf die Gesundheit und möglicher Weise das Leben von Menschen. Die Selbstsicherheit der Täter war besonders groß. Letztlich haben sie das Softwaretool zur Entschlüsselung gratis zur Verfügung gestellt und sich als treusorgend dargestellt. Aber kein Cyber-Krimineller darf hier Dankbarkeit erwarten.

Bei Ransomware-Taktiken, die auf kritische Infrastrukturen zielen, gehen der Schaden und die Auswirkung leider weit über das Finanzielle hinaus. Der Angriff auf die Pipeline an der U.S.-Ostküste ist wahrscheinlich als Wendepunkt einzustufen: So sollen in den USA zukünftig Ransomware-Attacken mit Terrorismus gleichgestellt werden. Ich denke, dass uns Ransomware-Phänome in nächster Zeit noch verstärkt beschäftigen werden. Bei aller Sorge darf man aber nie die großen Potenziale der Digitalisierung übersehen und sollte Bedrohungen auch als Chancen begreifen. Wer seine Resilienz stärkt, wird das Positive im Digitalzeitalter weiterhin gut nützen können.

Interview: Gregor Wenda

FOTO: GREGOR WENDA